REMARKS

In a March 17, 2009, Office Action (hereinafter "Office Action"), Claims 1, 4, 5, 7-9, and 32-36 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,002,994 issued to Lane et al. (hereinafter "Lane"). Claims 10-31, 38-50, and 52-58 were rejected under 35 U.S.C. § 103(a) as being obvious in view of Lane and in further view of U.S. Patent No. 6229429 issued to Horon et al. (hereinafter "Horon"). Applicants respectfully submit that the rejected claims of the present application are not anticipated and are non-obvious over the cited references, alone or in combination, because the cited references fail to teach or suggest characterizing, rule identification, and processing of incoming monitoring device data, as recited in each of the independent claims of the present application.

Claims 1, 4, 5, 7-9, and 32-36

The Office Action rejected Claims 1, 4, 5, 7-9, and 32-36 under 35 U.S.C. § 102(b) as being anticipated by Lane. Applicants respectfully disagree. Even though applicants respectfully disagree with the grounds of the rejection, clarifying amendments have been made to each of the independent claims to fairly clarify and distinguish each of these independent claims from the cited reference.

Claims 1 and 34

For purposes of this discussion, independent Claims 1 and 34 of the present application will be discussed together because the same or similar distinguishing elements over Lane are recited in each of these claims. In this regard, Claim 1, as amended recites the following:

> 1. In an integrated information system including a central server in communication with premises servers that are associated with two or more geographically distinct sites, a method for processing monitoring device data, the method comprising:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

obtaining monitoring device data at the premises servers that are associated with the two or more geographically distinct sites, wherein the monitoring device data corresponds to two monitoring devices with at least one monitoring device at each geographically distinct site wherein the monitoring device data is obtained continuously;

at the premises servers, characterizing the monitoring device data as at least one of asset data, resource data, and event data;

transmitting the monitoring device data and characterization data from the premises servers to the central server;

obtaining one or more monitoring rules at the central server corresponding to the at least one monitoring device, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation and wherein obtaining one or more rules includes at least one of:

obtaining asset rules if the monitoring device data is characterized as asset data;

obtaining resource rules if the monitoring device data is characterized as resource data; and

obtaining device rules if the monitoring device data is characterized as event data;

processing the monitoring device data at the central server according to the monitoring rules to determine whether a rule violation occurred wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices;

wherein processing the monitoring device data according to the rules includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and

generating an output corresponding to the processing of the monitoring device data, wherein the output indicates whether a rule violation occurred;

characterizing the monitoring device data as asset data, resource data or event data;

wherein asset data includes data from an identifiable object that is not capable of independent action;

wherein resource data includes data from an object capable of independent action; and

wherein event data includes data from a device having a defined state.

Similarly, Claim 34 recites the following:

34. A system for implementing an integrated information system, the system comprising:

one or more monitoring devices corresponding to two or more geographically distinct sites organized according to geographic criteria and operable to continuously transmit monitoring device data;

one or more premises servers operable to obtain the monitoring device data from the one or more monitoring devices, characterize the monitoring device data as at least one of asset data, resource data, and event data, transmit the monitoring device data and characterization data to the central processing server;

a central processing server, the central processing server operable to continuously obtain the monitoring device data originating from at least one monitoring device at each of the two or more geographically distinct sites;

wherein the central processing server processes the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria, wherein the central processing server generates an output corresponding to the processing, wherein the output reflects the results of processing the monitoring device data according to the rules;

wherein the processing of monitoring device data performed by the central processing server includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and

wherein the processing of monitoring device data performed by the central processing server includes at least one of:

obtaining asset rules if the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action;

obtaining resource rules if the monitoring device data is characterized as resource data from an object capable of independent action;

obtaining device rules if the monitoring device data is characterized as event data from a device having a defined state; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

Each of these independent claims recites elements relating to characterizing incoming monitoring device data. In this regard, the independent Claims 1 and 34 recite "at the premises servers, characterizing the monitoring device data as at least one of asset data, resource data, and

event data" (Claim 1); "characterizes the monitoring device data as at least one of asset data, resource data, and event data, transmit the monitoring device data and characterization to the central processing server" (Claim 34). Once the data originating from a monitoring device is characterized, logic is implemented to identify the appropriate rule type and determine how the monitoring device data will be processed. In this regard, independent Claims 1 and 34 recite "obtaining one or more monitoring rules . . . wherein obtaining one or more rules includes at least one of obtaining asset rules if the monitoring device data is characterized as asset data; obtaining resource rules if the monitoring device data is characterized as resource data; and obtaining device rules if the monitoring device data is characterized as event data" (Claim 1); "wherein the processing of the monitoring device data performed by the central processing server includes at least one of: obtaining asset rules if the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action; obtaining resource rules if the monitoring device data is characterized as resource data from an object capable of independent action; obtaining device rules if the monitoring device data is characterized as event data from a device having a defined state" (Claim 34). Simply stated, the manner in which the incoming monitoring device data is characterized for subsequent rule identification and processing, as reflected in Claims 1 and 34, is not taught in Lane alone or in combination with the other cited references.

The Office Action asserts that Lane teaches a method of processing device data in an integrated information system. Moreover, the Office Action asserts that Lane teaches characterizing the device data as asset data, resource data, or event data, as recited in Claims 1 and 34, and references Lane at Col. 7, lines 36-61 and Col. 10, lines 15-20 as teaching these claim elements. However, the cited portions of Lane teach a security system in which motion detectors are divided into various zones and a monitoring subroutine in which the status of a

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

door, with regard to being opened or closed, is monitored. However, this disclosure in Lane does not teach characterizing incoming monitoring device data and identifying the appropriate rule to process the data based on this characterization.

As described above, Lane fails to teach or suggest an integrated information system in which an incoming monitoring device is characterized and corresponding rules are identified and used to process the monitoring device. Since Lane and the other cited references fail to teach each element recited in Claims 1 and 34, applicants respectfully request withdrawal of the 35 U.S.C. § 102 rejection of these claims.

Claims 4, 5, 7-9, 32, 33, 35, and 36

Claims 4, 5, 7-9, 32, 33, 35, and 36 depend on independent Claims 1 and 34, respectively. As discussed above, Lane fails to teach or suggest an integrated information system as recited in each of these independent claims. Accordingly, for at least their dependency on Claims 1 and 34, Claims 4, 5, 7-9, 32, 33, 35, and 36 are also allowable.

Claims 59-68

Claims 59-68 have been added in the present amendment. In this regard, Claim 59 includes claim elements that mirror independent Claim 34, having premises and central processing means for characterizing and processing the monitoring device data. As described above with reference to Claims 1 and 34, Lane and the other cited references do not describe an integrated information system in which computing devices or means characterize the monitoring device data and identify an appropriate rule for processing the monitoring device data as recited in Claim 59. Accordingly, applicants submit that for the same reasons as described above with reference to independent Claims 1 and 34, new Claim 59 is also allowable.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Since the dependent Claims 60-68 carry each and every element of a claim with allowable subject matter from which they depend (Claim 59), these claims are all also allowable.

Conclusion

In view of the foregoing amendments, applicants respectfully submit that all the claims in the application are allowable. Consequently, early and favorable action allowing these claims and passing the application to issue is respectfully solicited.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

CJF:lal